Formalizing Perfectoid Fields

Kenny Lau

Imperial College London

January 6, 2021

A Tale of Two Cities

A number field is a finite extension of $\mathbb{Q}$, such as:

- $\mathbb{Q}$
- $\mathbb{Q}(i)$
- $\mathbb{Q}\left(\sqrt{2}\right)$

These fields have characteristic 0 and are central to number theory.

A function field is a finite extension of $\mathbb{F}_q(t)$, such as:

- $\mathbb{F}_{37}(t)$
- $\mathbb{F}_{37^2}(t)$
- $\mathbb{F}_{37}(\sqrt{t})$

These fields have characteristic p and arise from projective curves over finite fields.

A Tale of Two Cities — Completion

Given a prime number p, we can form the field of p-adic numbers $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ under the p-adic norm $\|\cdot\|_p$.

Recall that $\|p\|_p = p^{-1}$.

Similiarly, we can complete $\mathbb{F}_p(t)$ under the norm $\|\cdot\|_t$ to form $\mathbb{F}_p(\!(t)\!)$.

Recall that $\|t\|_t = p^{-1}$.

A Tale of Two Cities — Ring of Integers

The ring of integers of $\mathbb{Q}_p$ is:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$$

It has a unique maximal ideal $p\mathbb{Z}_p$, and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Similarly, the ring of integers of $\mathbb{F}_p(\!(t)\!)$ is:

$$\mathbb{F}_p[\![t]\!] = \{x \in \mathbb{F}_p(\!(t)\!) : \|x\|_t \leq 1\}$$

It has a unique maximal ideal $t\mathbb{F}_p[\![t]\!]$, and $\mathbb{F}_p[\![t]\!]/t\mathbb{F}_p[\![t]\!] \cong \mathbb{F}_p$.

Function Field Analogy on nLab

	number fields ("function fields of curves over F1")	function fields of curves over finite fields $\mathbb{F}_q$ (arithmetic curves)	Riemann surfaces/complex curves
affine and projective line			
	$\mathbb{Z}$ (integers)	$\mathbb{F}_q[z]$ (polynomials, function algebra on affine line $\mathbb{A}^1_{\mathbb{F}_q}$)	$\mathcal{O}_{\mathbb{C}}$ (holomorphic functions on complex plane)
	$\mathbb{Q}$ (rational numbers)	$\mathbb{F}_q(z)$ (rational functions)	meromorphic functions on complex plane
	p (prime number/non-archimedean place)	$x \in \mathbb{F}_p$	$x \in \mathbb{C}$
	∞ (place at infinity)		∞
	$\mathrm{Spec}(\mathbb{Z})$ (Spec(Z))	$\mathbb{A}^1_{\mathbb{F}_q}$ (affine line)	complex plane
	$\mathrm{Spec}(\mathbb{Z}) \cup \mathrm{place}_\infty$	$\mathbb{P}_{\mathbb{F}_q}$ (projective line)	Riemann sphere
	$\partial_p \coloneqq \frac{(-)^p-(-)}{p}$ (Fermat quotient)	$\frac{\partial}{\partial z}$ (coordinate derivation)	"
	genus of the rational numbers = 0		genus of the Riemann sphere = 0
formal neighbourhoods			
	$\mathbb{Z}_p$ (p-adic integers)	$\mathbb{F}_q[[t-x]]$ (power series around x)	$\mathbb{C}[[z-x]]$ (holomorphic functions on formal disk around x)

Function Field Analogy on nLab

	number fields ("function fields of curves over F1")	**function fields of curves over finite fields $\mathbb{F}_q$ (arithmetic curves)**	**Riemann surfaces/complex curves**
	$\mathrm{Spf}(\mathbb{Z}_p) \underset{\mathrm{Spec}(\mathbb{Z})}{\times} X$ ("p-arithmetic jet space" of X at p)		formal disks in X
	$\mathbb{Q}_p$ (p-adic numbers)	$\mathbb{F}_q((z-x))$ (Laurent series around x)	$\mathbb{C}((z-x))$ (holomorphic functions on punctured formal disk around x)
	$\mathbb{A}_{\mathbb{Q}} = \prod'_{p\ \mathrm{place}} \mathbb{Q}_p$ (ring of adeles)	$\mathbb{A}_{\mathbb{F}_q((t))}$ (adeles of function field)	$\prod'_{x \in \mathbb{C}} \mathbb{C}((z-x))$ (restricted product of holomorphic functions on all punctured formal disks, finitely of which do not extend to the unpunctured disks)
	$\mathbb{I}_{\mathbb{Q}} = \mathrm{GL}_1(\mathbb{A}_{\mathbb{Q}})$ (group of ideles)	$\mathbb{I}_{\mathbb{F}_q((t))}$ (ideles of function field)	$\prod'_{x \in \mathbb{C}} \mathrm{GL}_1(\mathbb{C}((z-x)))$
theta functions			
	Jacobi theta function		
zeta functions			
	Riemann zeta function	Goss zeta function	
branched covering curves			
	K a number field ($\mathbb{Q} \hookrightarrow K$ a possibly ramified finite dimensional field extension)	K a function field of an algebraic curve Σ over $\mathbb{F}_p$	K_Σ (sheaf of rational functions on complex curve Σ)

Function Field Analogy on nLab

	number fields ("function fields of curves over F1")	**function fields of curves over finite fields $\mathbb{F}_q$ (arithmetic curves)**	**Riemann surfaces/complex curves**
	$\mathcal{O}_K$ (ring of integers)		$\mathcal{O}_\Sigma$ (structure sheaf)
	$\mathrm{Spec}_{\mathrm{an}}(\mathcal{O}_K) \to \mathrm{Spec}(\mathbb{Z})$ (spectrum with archimedean places)	Σ (arithmetic curve)	$\Sigma \to \mathbb{C}P^1$ (complex curve being branched cover of Riemann sphere)
	$\frac{(-)^p - \Phi(-)}{p}$ (lift of Frobenius morphism/Lambda-ring structure)	$\frac{\partial}{\partial z}$	"
	genus of a number field	genus of an algebraic curve	genus of a surface
formal neighbourhoods			
	v prime ideal in ring of integers $\mathcal{O}_K$	$x \in \Sigma$	$x \in \Sigma$
	K_v (formal completion at v)		$\mathbb{C}((z_x))$ (function algebra on punctured formal disk around x)
	$\mathcal{O}_{K_v}$ (ring of integers of formal completion)		$\mathbb{C}[[z_x]]$ (function algebra on formal disk around x)
	$\mathbb{A}_K$ (ring of adeles)		$\prod'_{x\in\Sigma} \mathbb{C}((z_x))$ (restricted product of function rings on all punctured formal disks around all points in Σ)
	$\mathcal{O}$		$\prod_{x\in\Sigma} \mathbb{C}[[z_x]]$ (function ring on all formal disks around all points in Σ)

Function Field Analogy on nLab

	number fields ("function fields of curves over F1")	function fields of curves over finite fields $\mathbb{F}_q$ (arithmetic curves)	Riemann surfaces/complex curves
	$\mathbb{I}_K = \mathrm{GL}_1(\mathbb{A}_K)$ (group of ideles)		$\prod'_{x \in \Sigma} \mathrm{GL}_1(\mathbb{C}((z_x)))$
Galois theory			
	Galois group	"	$\pi_1(\Sigma)$ fundamental group
	Galois representation	"	flat connection ("local system") on Σ
class field theory			
	class field theory	"	geometric class field theory
	Hilbert reciprocity law	Artin reciprocity law	Weil reciprocity law
	$\mathrm{GL}_1(K)\backslash\mathrm{GL}_1(\mathbb{A}_K)$ (idele class group)	"	
	$\mathrm{GL}_1(K)\backslash\mathrm{GL}_1(\mathbb{A}_K)/\mathrm{GL}_1(\mathcal{O})$	"	$\mathrm{Bun}_{\mathrm{GL}_1}(\Sigma)$ (moduli stack of line bundles, by Weil uniformization theorem)
non-abelian class field theory and automorphy			
	number field Langlands correspondence	function field Langlands correspondence	geometric Langlands correspondence

Function Field Analogy on nLab

	number fields ("function fields of curves over F1")	function fields of curves over finite fields $\mathbb{F}_q$ (arithmetic curves)	Riemann surfaces/complex curves
	$\mathrm{GL}_n(K)\backslash \mathrm{GL}_n(\mathbb{A}_K)//\mathrm{GL}_n(\mathcal{O})$ (constant sheaves on this stack form unramified automorphic representations)	"	$\mathrm{Bun}_{\mathrm{GL}_n(\mathbb{C})}(\Sigma)$ (moduli stack of bundles on the curve Σ, by Weil uniformization theorem)
	Tamagawa-Weil for number fields	Tamagawa-Weil for function fields	
theta functions			
	Hecke theta function		functional determinant line bundle of Dirac operator/chiral Laplace operator on Σ
zeta functions			
	Dedekind zeta function	Weil zeta function	zeta function of a Riemann surface/of the Laplace operator on Σ
higher dimensional spaces			
zeta functions	Hasse-Weil zeta function		

***analogies* in the *Langlands program*:**

The Question

How can we connect $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$?
Or, more precisely, how do **extensions** of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ relate to each other?

First Attempt

We will try to use the fact that the rings of integers of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are linked via the isomorphism $\mathbb{Z}_p/p \cong \mathbb{F}_p[\![t]\!]/t$.

$$\begin{tikzcd}
\mathbb{Q}_p \arrow[r, "\text{ring of integers}"] & \mathbb{Z}_p \arrow[r] & \mathbb{Z}_p/p \arrow[d, dash, "\cong"] \\
\mathbb{F}_p((t)) \arrow[r, "\text{ring of integers}"] & \mathbb{F}_p[\![t]\!] \arrow[r] & \mathbb{F}_p[\![t]\!]/t
\end{tikzcd}$$

But the problem is that $\mathbb{Q}_3(\sqrt{3})$ and $\mathbb{Q}_3(\sqrt{-3})$ both produce $\mathbb{F}_3[x]/(x^2)$:

$$\begin{tikzcd}
\mathbb{Q}_3(\sqrt{3}) \arrow[r, "\text{r.o.i.}"] & \mathbb{Z}_3[\sqrt{3}] = \mathbb{Z}_3[x]/(x^2-3) \arrow[r] & \mathbb{F}_3[x]/(x^2) \arrow[d, dash, "\cong"] \\
\mathbb{Q}_3(\sqrt{-3}) \arrow[r, "\text{r.o.i.}"] & \mathbb{Z}_3[\sqrt{-3}] = \mathbb{Z}_3[x]/(x^2+3) \arrow[r] & \mathbb{F}_3[x]/(x^2)
\end{tikzcd}$$

The Solution

The solution is to adjoin the $(p^n)^{\text{th}}$ roots:

$$\begin{tikzcd}
\mathbb{Q}_p\left(p^{1/p^\infty}\right) \arrow[r, "\text{ring of integers}"] & \mathbb{Z}_p\left[p^{1/p^\infty}\right] \arrow[r] & \mathbb{Z}_p\left[p^{1/p^\infty}\right]/p \arrow[d, dash, "\cong"] \\
\mathbb{F}_p(\!(t)\!)\left(t^{1/p^\infty}\right) \arrow[r, "\text{ring of integers}"] & \mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right] \arrow[r] & \mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]/t
\end{tikzcd}$$

Then this works, and extensions of $\mathbb{Q}_p\left(p^{1/p^\infty}\right)$ correspond to extensions of $\mathbb{F}_p(\!(t)\!)\left(t^{1/p^\infty}\right)$, unlike in the case with $\mathbb{Q}_p$ and $\mathbb{F}_p(\!(t)\!)$.

What is a perfectoid field?

- $\mathbb{Q}_p$ comes with a norm $\|\cdot\|_p$ with $\|p\|_p = \frac{1}{p}$.
- Adjoin $(p^n)^{\text{th}}$ roots of p and end up with:

$$\mathbb{Q}_p\left(p^{1/p^\infty}\right) := \bigcup_{n=0}^{\infty} \mathbb{Q}_p\left(p^{1/p^n}\right)$$

- Extend the norm $\|\cdot\|_p$ to $\mathbb{Q}_p\left(p^{1/p^\infty}\right)$ with:

$$\left\|p^{1/p^n}\right\|_p = p^{-1/p^n}$$

What is a perfectoid field?

- The ring of integers of $\mathbb{Q}_p$ is $\mathbb{Z}_p$.
  It is characterized by:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$$

- Similarly, the ring of integers of $\mathbb{Q}_p\left(p^{1/p^\infty}\right)$ is:

$$\mathbb{Z}_p\left[p^{1/p^\infty}\right] := \bigcup_{n=0}^{\infty} \mathbb{Z}_p\left[p^{1/p^n}\right]$$

- Then $\mathbb{Z}_p\left[p^{1/p^\infty}\right]/p$ is a ring of characteristic p for which the Frobenius homomorphism $x \mapsto x^p$ is surjective (cf. the definition of perfect fields where the Frobenius homomorphism is bijective).

Tilting

Recall our situation:

$$\begin{tikzcd}
\overline{\mathbb{Q}_p\left(p^{1/p^\infty}\right)} \arrow[r, "\text{ring of integers}"] & \overline{\mathbb{Z}_p\left[p^{1/p^\infty}\right]} \arrow[r] & \mathbb{Z}_p\left[p^{1/p^\infty}\right]/p \arrow[d, dash, "\cong"] \\
\overline{\mathbb{F}_p((t))\left(t^{1/p^\infty}\right)} \arrow[r, "\text{ring of integers}"] & \overline{\mathbb{F}_p[[t]]\left[t^{1/p^\infty}\right]} \arrow[r] & \mathbb{F}_p[[t]]\left[t^{1/p^\infty}\right]/t
\end{tikzcd}$$

where we have completed the fields under the respective norms.

Note that for example the completion of $\mathbb{F}_p[[t]]\left[t^{1/p^\infty}\right]$ contains:

$$\sum_{n=0}^{\infty} t^{n+1/p^n}$$

But the quotients are the same.

Tilting

It turns out that one can "construct" $\overline{\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]}$ from $\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]/t$ by:

$$\overline{\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]} = \varprojlim_{x \mapsto x^p} \left(\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]/t\right)$$

not unlike how:

$$\mathbb{Z}_p = \varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right)$$

and:

$$\mathbb{F}_p[\![t]\!] = \varprojlim \left(\mathbb{F}_p[t]/t^n\right)$$

Tilting

So in some sense $\overline{\mathbb{F}_p((t))\left(t^{1/p^\infty}\right)}$ can be constructed from $\overline{\mathbb{Q}_p\left(p^{1/p^\infty}\right)}$ by the following procedure:

$$\begin{tikzcd}
\overline{\mathbb{Q}_p\left(p^{1/p^\infty}\right)} \arrow[r, "\text{ring of integers}"] & \overline{\mathbb{Z}_p\left[p^{1/p^\infty}\right]} \arrow[r] & \mathbb{Z}_p\left[p^{1/p^\infty}\right]/p \arrow[d, "\cong"] \\
\overline{\mathbb{F}_p((t))\left(t^{1/p^\infty}\right)} & \overline{\mathbb{F}_p[[t]]\left[t^{1/p^\infty}\right]} \arrow[l, "\text{field of fractions}"'] & \mathbb{F}_p[[t]]\left[t^{1/p^\infty}\right]/t \arrow[l, "\varprojlim_{x \mapsto x^p}"']
\end{tikzcd}$$

We say that $\overline{\mathbb{F}_p((t))\left(t^{1/p^\infty}\right)}$ is the tilt of $\overline{\mathbb{Q}_p\left(p^{1/p^\infty}\right)}$.

Perfection

Recall:

$$\overline{\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]} = \varprojlim_{x \mapsto x^p} \left(\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]/t\right)$$

So we say that $\overline{\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]}$ is the perfection of $\mathbb{F}_p[\![t]\!]\left[t^{1/p^\infty}\right]/t$.

We also have:

$$\overline{\mathbb{F}_p(\!(t)\!)\left(t^{1/p^\infty}\right)} = \varprojlim_{x \mapsto x^p} \overline{\mathbb{Q}_p\left(p^{1/p^\infty}\right)}$$

But this is only as monoids, i.e. the isomorphism does not preserve addition. We say that $\overline{\mathbb{F}_p(\!(t)\!)\left(t^{1/p^\infty}\right)}$ is the monoid-perfection of $\overline{\mathbb{Q}_p\left(p^{1/p^\infty}\right)}$.

Formalization — Ring of Integers

What do we mean by:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\|_p \leq 1\}$$

What if we define $\mathbb{Z}_p$ differently?
How can we still relate $\mathbb{Z}_p$ and $\mathbb{Q}_p$?
Answer: Characteristic predicate.

`src/ring_theory/valuation/integers.lean` in mathlib commit a6633e5:

```
/-- Given a valuation v : R → Γ₀ and a ring homomorphism O →+* R, we say that O is the integers of v
if f is injective, and its range is exactly `v.integer`. -/
structure integers : Prop :=
(hom_inj : function.injective (algebra_map O R))
(map_le_one : ∀ x, v (algebra_map O R x) ≤ 1)
(exists_of_le_one : ∀ ⦃r⦄, v r ≤ 1 → ∃ x, algebra_map O R x = r)
```

Formalization — Ring of Integers

ibid.:

```
/-- The ring of integers under a given valuation is the subring of elements with valuation ≤ 1. -/
def integer : subring R :=
{ carrier := { x | v x ≤ 1 },
  one_mem' := le_of_eq v.map_one,
  mul_mem' := λ x y hx hy, trans_rel_right (≤) (v.map_mul x y) (mul_le_one' hx hy),
  zero_mem' := trans_rel_right (≤) v.map_zero zero_le_one',
  add_mem' := λ x y hx hy, le_trans (v.map_add x y) (max_le hx hy),
  neg_mem' := λ x hx, trans_rel_right (≤) (v.map_neg x) hx }
```

ibid.:

```
theorem integer.integers : v.integers v.integer :=
{ hom_inj := subtype.coe_injective,
  map_le_one := λ r, r.2,
  exists_of_le_one := λ r hr, ⟨⟨r, hr⟩, rfl⟩ }
```

Formalization — Perfection

`src/ring_theory/perfection.lean` in mathlib commit a6633e5:

```
/-- The perfection of a ring `R` with characteristic `p`,
defined to be the projective limit of `R` using the Frobenius maps `R → R`
indexed by the natural numbers, implemented as `{ f : ℕ → R | ∀ n, f (n + 1) ^ p = f n }`. -/
def ring.perfection (R : Type u₁) [comm_semiring R]
  (p : ℕ) [hp : fact p.prime] [char_p R p] :
  subsemiring (ℕ → R) :=
{ zero_mem' := λ n, zero_pow $ hp.pos,
  add_mem' := λ f g hf hg n, (frobenius_add R p _ _).trans $ congr_arg2 _ (hf n) (hg n),
  .. monoid.perfection R p }
```

ibid.:

```
/-- A perfection map to a ring of characteristic `p` is a map that is isomorphic
to its perfection. -/
@[nolint has_inhabited_instance] structure perfection_map (p : ℕ) [fact p.prime]
  {R : Type u₁} [comm_semiring R] [char_p R p]
  {P : Type u₂} [comm_semiring P] [char_p P p] [perfect_ring P p] (π : P →+* R) : Prop :=
(injective : ∀ ⦃x y : P⦄, (∀ n, π (pth_root P p ^[n] x) = π (pth_root P p ^[n] y)) → x = y)
(surjective : ∀ f : ℕ → R, (∀ n, f (n + 1) ^ p = f n) →
  ∃ x : P, ∀ n, π (pth_root P p ^[n] x) = f n)
```